NASA OIG News

Highlights in this Issue

Lessons learned and advice
Snapshot of current activities
What's new
Inside the OIG

LESSONS LEARNED AND ADVICE

Conflicts/Appearances

To avoid even the appearance of improper use of public office for private gain and to preserve the integrity of NASA decision making, NASA employees should be careful of their involvement in contracts or grants when a current or prospective contractor or grantee employs a family member. In certain situations, NASA employees may have to recuse themselves from an acquisitions process. Employees should immediately consult the Agency or installation ethics official (located in installation chief counsel offices) when confronted with such situations.

Timecard Fraud

As the result of a recent NASA OIG criminal investigation, a former Goddard Space Flight Center employee was sentenced on a charge of theft of Government funds for falsifying timecards by adding hours not worked. The Agency has clear rules governing the approval process for overtime and compensatory time. Obviously, these rules should be closely followed. In addition, NASA supervisors should be careful to monitor and verify employee use of such extra work time, particularly long periods of overtime and compensatory time.

Hard Drive Sensitive Information

Inspections staff members are following up on the corrective actions implemented by NASA in response to an OIG inspection in 1997 that revealed electronic information, including sensitive data, remained on the hard drives of computers that were considered ready to be excessed. The NASA Chief Information Officer and every NASA Center have existing policies and guidelines to thoroughly and completely clear computer hard drives before they are excessed. NASA managers, particularly those responsible for sensitive and controlled information (e.g., personnel, procurement, security, etc.) should take steps to assure that electronic information in hard drives is completely wiped clear before a hard drive leaves their work area.

SNAPSHOT OF ACTIVITIES

Audits

During the past 18 months, the Information Assurance Directorate (IAD) has audited the adequacy of security and internal controls for selected major NASA information technology systems and their associated data centers. The IAD recommended that NASA improve physical security, environmental protection, and control over computing operations. In addition, the audits disclosed that disaster recovery capabilities are lacking. We have issued nine final reports, and three additional reports are being drafted.

Investigations

The OIG remote sensing initiative was presented at the Northeast Environmental Enforcement Project's (NEEP) conference in Charlottesville, VA, in November. The NEEP is comprised of environmental enforcement officials from 13 states, Canada, and several Federal law enforcement agencies. The presentation sparked considerable interest and discussion. The OIG remote sensing team also initiated discussions with the Environmental Protection Agency's Center for Strategic Environmental Enforcement to work together to use NASA remote sensing technology to preserve and protect the environment.

See the December 7, 1998, *Federal Times* article, "NASA Explores Using Crime-Fighting Satellites," for more information on this topic.

Legal

The OIG Attorney-Advisor recently prepared an article entitled "Remote Sensing and the Fourth Amendment: A New Law Enforcement Tool?" The article explores the legal implications of using remote sensing as an investigative tool in law enforcement. To read the full article, visit the OIG web site: http://www.hq.nasa.gov/office/oig/hq/remote4.html.

The U.S. Supreme Court has granted an order of certiorari in the case of *NASA v. Federal Labor Relations Authority*. This means that the Supreme Court will hear the case and decide whether OIG agents are "representatives of the agency" for the purpose of the Federal labor relations statute.

WHAT'S NEW

The audit staff issued reports on the NASA science research institutes, information technology capital planning and investment control, Space Station configuration management, X-33 funding issues, commercial use of the Santa Susana Field Laboratory, general-purpose vehicles acquisition and use, and single-source suppliers for critical items.

NASA OIG criminal investigations resulted in:
- a NASA HQ employee pled guilty to one count of theft and conversion of Government funds by falsely claiming travel expenses not incurred.
- a NASA HQ employee pled guilty to one count of grand theft for pawning a Government computer.

The IAIA staff routed a lessons learned report to the NASA Chief Information Officer and Security communities on a network intrusion at a NASA installation.

The full text of most of these and other NASA OIG reports and news releases can be found on our web site at: *http://www.hq.nasa.gov/office/oig/hq*.

INSIDE THE OIG

We are pleased to introduce the following new staff members:

Vera Garrant, A-133 Program Manager, has joined the staff of the Assistant Inspector General for Auditing. Vera will conduct quality control reviews of the independent auditors' working papers that support audits conducted in accordance with the Single Audit Act and OMB Circular A-133, "Audits of States, Local Governments and Non-Profit Organizations." She will conduct reviews of institutions for which NASA has cognizance and oversight.

Paul Shawcross, Aerospace Technologist – Technical Management, recently joined the OIG IAIA team. Paul previously served as a senior analyst with the National Research Council. In addition to leading technical evaluations of NASA activities, Paul will support the entire OIG staff with advice and consultation on engineering and other technical issues.